AMENDMENTS TO THE CLAIMS:

Without prejudice, this listing of the claims replaces all prior versions and listings of the claims in the present application:

LISTING OF CLAIMS:

Claims 1 to 12. (Canceled).

13. (Currently Amended) A method for encrypting data according to an asymmetrical method using a processor, based on a factorization problem, comprising:

providing a public key to the processor; and

providing a private key to the processor; wherein the public key includes composite number n; the [[~~a~~]] private key is made up of the factorization of n; a message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 *and* m_2; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$, c_1 and c_2 being integral numbers; $f(m)=(f_1(m), f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n, it thus [[~~thereby~~]] being possible to retrieve the original message from the encrypted information $c = (c_1, c_2)$,

wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, [[~~particularly~~]] in the case of prime numbers of form 3 mod [[~~rood~~]] 4, can be communicated by 2 bits per iteration step.

14. (Canceled).

15. (Canceled).

16. (Previously Presented) The method of claim 13, wherein general iterations $f_1=(k_1 \bullet m_1+k_2 \bullet m_2) \bmod n$ as well as $f_2=k_3 \bullet m_1 \bullet m_2 \bmod n$ are used, constants being part of the public key.

17. (Previously Presented) The method of claim 13, wherein the composite number n as public key contains more than two factors.

18. (Previously Presented) The method of claim 13, wherein the message is now made up of an N-tuple $m=(m_1...m_N)$, the formula for the Lth iteration step using dependencies of N values in each iteration step.

19. (Previously Presented) The method of claim 18, wherein the multivaluedness is resolved by additional bits that are derived from the values obtained in each iteration.

20. (Previously Presented) The method of claim 13, wherein the multivaluedness is resolved by redundancy in the transmitted data.

21. (Currently Amended) A method for generating a signature using a processor, comprising:

generating using the processor a signature by interchanging the encryption and decryption steps, including functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; wherein the public key includes a composite number n; the [[~~a~~]]private key being made up of the factorization of n; a message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 *and* m_2; an encryption function $f(x)$ is iterated a total of L times, with $c=(c_1, c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n, it [[~~thereby~~]]thus being possible to retrieve the original message from the encrypted information c[[=]] $= (c_1, c_2)$, c_1 and c_2 being integral numbers; wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, [[~~particularly~~]]in the case of prime numbers of form 3 mod [[~~rood~~]]4, can be communicated by 2 bits per iteration step.

22. (Canceled).

23. (Currently Amended) A data carrier storage for a computer, comprising:

storage of a software for the computer, the software being instructions configured to be executed by the computer, the instructions which, when executed by the computer, cause the performance of functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; wherein the public key includes a composite number n; the [[~~a~~]] private key being made up of the factorization of n; a message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 *and* m_2; an

encryption function $f(x)$ is iterated a total of L times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n, it [[~~thereby~~]]thus being possible to retrieve the original message from the encrypted information c [[=]] = (c1, c2), c_1 and c_2 being integral numbers; wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol which, [[~~particularly~~]]in the case of prime numbers of form 3 mod [[~~rood~~]]4, can be communicated by 2 bits per iteration step.

24. (Currently Amended) A computer system, comprising: [[,]]

a device that executes a method, the method having software for a computer, comprising functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; wherein the public key includes a composite number n; the private key being made up of the factorization of n; a message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 and m_2; an encryption function $f(x)$ being iterated a total of L times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n, it thus [[~~thereby~~]]being possible to retrieve the original message from the encrypted information c[[=]]= (c1, c2), c_1 and c_2 being integral numbers; wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i to obtain a set of roots and by calculating a parity and a Jacobi symbol, [[~~particularly~~]]in the case of prime numbers of form 3 [[~~rood~~]]mod 4, can be communicated by 2 bits per iteration step.

25. (Previously Presented) The method of claim 13, wherein n is a product of a plurality of large prime numbers.

26. (Previously Presented) The method of claim 25, wherein op_1 is an addition and op_2 is a multiplication.

27. (Previously Presented) The method of claim 13, wherein op_1 is an addition and op_2 is a multiplication.

28. (Previously Presented) The method of claim 21, wherein n is a product of a plurality of large prime numbers, and op_1 is an addition and op_2 is a multiplication.

29. (Canceled).

30. (Previously Presented) The method of claim 23, wherein n is a product of a plurality of large prime numbers, and op_1 is an addition and op_2 is a multiplication.

31. (Previously Presented) The method of claim 24, wherein n is a product of a plurality of large prime numbers, and op_1 is an addition and op_2 is a multiplication.